firm, and it is also confirmed that the IC card terminal **12**, to which this IC card **11** is being loaded, is also authentic. After confirmation of the authenticity between IC card **11** and IC card terminal **12** according to the invention, the cardholder is identified by a normal "PIN" check before a transaction with the IC card can be executed.

If in step **S4**, decryption data "D-PAN" decrypted in the card terminal **12** and data "PAN" previously stored in IC card **11** are not coincident with each other, IC card terminal **12**, to which the present IC card **11** is being loaded, is highly likely to be unauthentic. Then the system goes to step **S8**, where card data transfer operation with card terminal **12** is immediately interrupted. Consequently, if IC card terminal **12** is unauthentic, or altered, this can be recognized before the actual transaction starts with the IC card, thus preventing possible problems.

Further, if in step **S6**, three sets of data "D-PAN", "D-CHN" and "D-EPD" decrypted in the card terminal **12** are not coindicent with three sets of data "PAN", "CHN" and "EPD" previously stored in IC card **11**, then it is highly likely that the IC card **11** being loaded to terminal **12** is unauthentic, so that data exchange with IC card **11** is inhibited in step **S9**. Thus, if the IC card **11** connected to terminal **12** is unauthentic, e.g., a forged one, such a fact can be recognized before the actual transaction with IC card commences, with the result that possible transaction trouble can be avoided.

It should be understood from the foregoing operations that the encrypted data "IA" previously stored in data memory **28** is utilized to judge the identity of the card terminal in the IC card, whereas three sets of data "PAN", "EPD" and "CHN" are used to judge the identification of the IC card in the card terminal.

Although the foregoing has been a description and illustration of specific embodiments of the invention, various modifications and changes thereto can be made by persons skilled in the art without departing from the scope of the invention.

In the above embodiment the "RSA" algorithm has been adopted for the encrypting system, but for example, it is also possible to introduce a "Data Encryption System" (DES).

Further, the unique data "PAN", "CHN" and "EPD" are not limited, but any other specific data may be employed.

While the invention has been described in the foregoing, both the data (PAN, CHN, EPD) unique to the IC card and the encrypted unique data (IA) obtained by encrypting the above data are previously stored in the IC card, the encrypted unique data is decrypted in the IC card terminal, and the decrypted data and unique data previously stored in the IC card are compared in both the IC card and the IC card terminal to confirm the authenticity or identities of both the IC card and the IC card terminal. Thus, it is possible to prevent illegal card transactions with, for instance, a forged IC card or a counterfeit or tempered IC card terminal.

Moreover, since the IC card does not require any encrypting circuit but merely stores the unique data and the data obtained by encrypting this unique data, it is possible to simplify the circuitry of the IC card and manufacture a low-cost IC card.

What is claimed is:

1. An identification system comprising:

IC card means;

IC card terminal means capable of electrically communicating with the IC card means when the IC card means is loaded thereon;

said IC card means including first memory means for storing at least data unique to said IC card means and encrypted unique data obtained by encrypting said unique data;

said IC card terminal means including decrypting means for decrypting said encrypted unique data stored in said first memory means to derive decrypted unique data;

said IC card means further including first comparing means for comparing said decrypted unique data sent from said IC card terminal means with said unique data stored in said first memory means so as to judge whether said unique data is coincident with said decrypted unique data; and

said IC card terminal further including second comparing means for comparing said decrypted unique data with said unique data stored in said first memory means and sent from said IC card means so as to judge whether said unique data is coincident with said decrypted unique data, thereby confirming identities of both said IC card means and said IC card terminal means.

2. An identification system as claimed in claim **1**, wherein, when the result of comparison by at least one of said first and second comparing means is non-coincident, subsequent communication between said IC card means and said IC card terminal means is interrupted.

3. An identification system as claimed in claim **2**, wherein said IC card terminal means further includes second memory means for storing key information for decryption, said decrypting means of said IC card terminal means decrypting said encrypted unique data stored in said first memory means on the basis of a "RSA" algorithm using said key information for decryption.

4. An identification system as claimed in claim **2**, wherein said unique data and encrypted unique data stored in said first memory means of said IC card means each comprise a plurality of different data information;

said IC card means includes first selecting means for selecting at least one of said plurality of unique data;

said IC card terminal means includes second selecting means for selecting at least one of a plurality of decrypted data decrypted by said decrypting means; and

said first comparing means compares said unique data with said decrypted data selected by said first and second selecting means so as to judge coincidence between said data.

5. An identification system as claimed in claim **4**, wherein, when the result of comparison by said first comparing means in said IC card means is coincident, said second comparing means of said IC card terminal means compares all of the unique data stored in said first memory means with all of the decrypted data decrypted by said decrypting means.

6. An identification system as claimed in claim **5**, wherein said unique data include data "PAN", "CHN" and "EPD", and said decrypted data is obtained by encrypting said data "PAN", "CHN" and "EPD" on the basis of an RSA algorithm.

* * * * *